UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,413	10/16/2003	Robert E. Cavanaugh	58895/P004US/10306553	8593

29053 7590 02/02/2010
FULBRIGHT & JAWORSKI L.L.P
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/02/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/687,413
Filing Date: October 16, 2003
Appellant(s): CAVANAUGH, ROBERT E.

Thomas Kelton
Reg. No. 54,214
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 11/11/2009 appealing from the Office action mailed on 6/12/09.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-8, 11-16, and 28-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Wexler et al. U.S. Pub. No. 20030229809 (hereinafter Wexler).

As per claim 1, Wexler discloses a security system for use in conjunction with data flowing from a first device to a second device being directed to said second device in accordance with a network address of said second device, said system comprising: a security device connected between said first and second devices (Wexler: [0009]: proxy server), said security device accepting packet data for bridging to said second device (Wexler: [0009]: handles packets), said security device operable for observing data flowing from said first device to said second device, said security device not itself having a network address or a physical address (Wexler: [0010]-[0011]: the proxy server does not have an IP address… proxy server changes contents of some of the packets it forwards; [0048]: optionally the network devices are not aware of the presence of the proxy server in **layer-2**/MAC), and configured to be inserted between said

first and said second device while a network connection is active (Wexler: [0009] lines 10-12: the transparent proxy server eliminates the need to configure network elements).

As per claim 2, Wexler discloses the system of claim 1. Wexler further discloses wherein said first device could be any device on the unsecured side of said security device, each said first device having a unique network address (Wexler: [0038]: source IP address), and wherein said second device could be any device on the secured side of said security device (Wexler: [0047] and figure 1: proxy protects local area network), each said second device having a unique network address (Wexler: [0038]: destination IP address).

As per claim 3, Wexler discloses the system of claim 2. Wexler further discloses wherein said security device maintains a list of addresses for which it has security responsibility and wherein said security device only observes those data packets containing the network addresses maintained in said list (Wexler: [0056]).

As per claim 4, Wexler discloses the system of claim 3. Wexler further discloses wherein said list includes addresses of both said first devices and said second devices (Wexler: [0056]: store IP addresses for security verification; [0062]: manages a list of expected packets; [0072]-[0073]: the tables include source and destination IP addresses).

As per claim 5, Wexler discloses the system of claim 1. Wexler further discloses wherein said observing comprises: a monitoring system for gathering information pertaining to the

operation of said second device (Wexler: [0072]: inbound and outbound reception table and transmission table); and a mechanism for modifying the flow of data into said security system depending upon said gathered information (Wexler: [0023]: modifying some fields of the packets).

As per claim 6, Wexler discloses the system of claim 5. Wexler further discloses wherein said gathered information is selected from the list containing: number of arriving packets in a particular time interval; the type of requests contained within given packets; the nature of the informational content of the packets; the sending identity of the packets; the destination of the packets; the traffic patterns formed by packets from specific sources; the number of arriving packets from specific sources; the correctness of the packets; certain data contained in one or more messages; and the type of file attached to a message (Wexler: [0072]-[0073]: storing information pertaining to operation of the proxy server; [0060]: functions of the proxy server).

As per claim 7, Wexler discloses the system of claim 5. Wexler further discloses wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits (Wexler: [0072]-[0073]: the tables are created for allowing communication between source and destination; [0104]: the table entry is erased upon time-out), and wherein said operational characteristics of said mechanism is modified in accordance with said set limits (Wexler: [0104]: when the entry is erased, session is closed).

As per claim 8, Wexler discloses a security device for use in a packet data network where packets are delivered from a sending location to a destination location based upon one or more destination network addresses associated with each packet (Wexler: [0009]: proxy server), said security device comprising: at least one NIC card for receiving data packets (Wexler: [0047]: inbound and outbound ports); a database for maintaining a list of destination network addresses to be secured by said device (Wexler: [0056]: proxy is configured with IP addresses of the entities in the local network); wherein said at least one NIC card is connected to said network at any point between a sending location and one or more destination locations (Wexler: [0047]: the inbound and outbound ports are connected to external router for Internet and edge router for local network), said NIC card maintained in promiscuous mode such that said security device can observe all data directed to any destination addresses maintained from time to time in said list (Wexler: [0056]: the proxy server operates in Promiscuous mode); wherein said security device is connected to said network without establishing a network address or a physical address for said security device (Wexler: [0009]: the proxy server is intercepts packets that is not directed to the proxy server; [0010]: the proxy server does not have an IP address; [0048]: optionally the network devices are not aware of the presence of the proxy server in layer-2/MAC); and wherein said security device can be moved from location to location on said network without changing any network settings (Wexler: [0009]: the transparent proxy server eliminates the need to configure network elements with the identity of the proxy server).

As per claim 11, Wexler discloses the device of claim 8. Wexler further discloses the method comprises a plurality of NIC cards all operating in said promiscuous mode (Wexler: [0056]: all packets are processed under Promiscuous mode).

As per claim 12, Wexler discloses the device of claim 11. Wexler further discloses wherein said security device has a zero network footprint while said NIC cards are in said promiscuous mode (Wexler: [0048]: the edge router and external router are not aware in layer 2 and layer 3 of the presence of proxy server).

As per claim 13, Wexler discloses the device of claim 12. Wexler further discloses wherein all of said NIC cards share the same destination list (Wexler: [0047]: inbound and outbound ports can transmit and receive data; [0068]: incoming and outgoing packets are verified according to destination IP address).

As per claim 14, Wexler discloses the device of claim 8. Wexler further discloses wherein said observing comprises: monitoring system for gathering information pertaining to the operation of said second device (Wexler: [0072]: inbound and outbound reception table and transmission table); and mechanism for modifying the flow of data into said security system depending upon said gathered information (Wexler: [0023]: modifying some fields of the packets).

As per claim 15, Wexler discloses the device of claim 14. Wexler further discloses wherein said gathered information is selected from the list containing: number of arriving packets in a particular time interval; the type of requests contained within given packets; the nature of the informational content of the packets; the sending identity of the packets; the destination of the packets; the traffic patterns formed by packets from specific sources; the number of arriving packets from specific sources; the correctness of the packets; certain data contained in one or more messages; and the type of file attached to a message (Wexler: [0072]-[0073]: storing information pertaining to operation of the proxy server; [0060]: functions of the proxy server).

As per claim 16, Wexler discloses the device of claim 15. Wexler further discloses wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits (Wexler: [0072]-[0073]: the tables are created for allowing communication between source and destination; [0104]: the table entry is erased upon time-out), and wherein said operational characteristics of said mechanism is modified in accordance with said set limits (Wexler: [0104]: when the entry is erased, session is closed).

As per claim 28, Wexler discloses a security device for connection in a data network ahead of a plurality of data destinations to be protected, each said destination identifiable by a unique network address (Wexler: [0056]: protect entities in local network), said security device comprising: means for accepting data packets from said network without said data packets being addressed to said security device (Wexler: [0009]: intercepts packets directed to destination IP

addresses); and means for passing accepted data packets to particular ones of said data destinations in accordance with destination addresses of said destinations to be detected and maintained for said security device (Wexler: [0048]: forwards packets to same IP addresses as they are received).

As per claim 29, Wexler discloses the device of claim 28. Wexler further discloses wherein said maintained destination addresses are stored in a database internal to said security device (Wexler: [0056]: store the IP addresses into the proxy server).

As per claim 30, Wexler discloses the device of claim 28. Wexler further discloses wherein said accepting means comprises: at least one network termination operating in a promiscuous mode (Wexler: [0056]).

(10) Response to Argument

Claims 1-7

Appellant argues that Wexler does not teach "said security device not itself having a network address or a physical address" because Wexler does not appear to teach a security device not having a physical address. Appellant further argues, "it does not appear to teach a security device not having a physical address...Accordingly, Wexler fails to teach the above-recited feature of claim 1 because Wexler explicitly teaches that its proxy server 22 includes a MAC address".

In response, the Examiner respectfully disagrees with Appellant because the claimed limitation, "said security device not itself having a network address or a physical address" , requires that "said security device not itself having" **either** "a network address" **or** "a physical address" and **not both!** . In view of that Appellant's claimed limitation "said security device not itself having a network address or a physical address" is interpreted as "said security device not itself having **a network address**".

Moreover, the Examiner would like to point out to Appellant that based on Appellant's Specification [0006-0007], the claimed limitation "said security device not itself having a network address or a physical address" is defined as "a method does not have a physical address **that is identifiable to any internal or external device, and is thus invisible and not available for** direct attack." In view of that Appellant argument is clearly contradict to Appellant 's own disclosure that Appellant's security device as disclosed clearly **does have a network address or a physical address** in which Appellant system is configure **to hide/mask its** network address or a physical address from external world/network to detect it.

As such, the Examiner asserts again that Wexler discloses its transparent proxy server 's network address or a physical address is configured such that other devices communicate with the transparent proxy server **are not aware of its network address or a physical address** (see Wexler Page 1, [0009], [0010], i.e. "the proxy server does not have an IP address, at least for the ports through which it performs its proxy task", [0013], i.e., " the proxy server does not have layer-3 address on its ports which connect to the two link...Alternatively, the proxy server does not have layer-3 (e.g., IP) address in any of its ports"; [0024], i.e., "a method of handling packets by a proxy server, including receiving, by the proxy server, one or more packets of a specific

session, not carrying an IP address of the proxy server in their IP destination address field; [0048], i.e., "Thus, edge router 26 and/or external router 28 are not aware, in layer-3, of the presence of proxy server 22 along path 24. Optionally, edge router 26 and/or external router 28 are not aware of the presence of proxy server 22 along the path 24, in layer-2"; [0049,. i.e., in some embodiments of the invention, ports 30 and 32 of proxy server 22 do not have layer-3, i.e., IP address." and [0051].

In conclusion, Appellant's argument is traversed in light of the above explanation.

Dependent claims 2-7 relies on the argument of claim 1. Therefore, claims 2-7 are rejected based on the same reason set forth above in rejecting claim 1.

Claims 8 and 11-16

Appellant argues that the prior art does not disclose "said security device is connected to said network without establishing a network address or a physical address for said security device." However, the examiner disagrees. As explained in previous section, Wexler discloses a transparent proxy server that is capable of communicating with network entities without having the network entities become aware of it (Wexler: [0009], [0048] and [0051]: no configuration is required/no address is established for network communication). Therefore, Appellant's argument on claims 8 and 11-16 is traversed in light of above explanation.

Claims 28-30

Claims 28-30 relies on the same argument as above. Therefore, argument on claims 28-30 is traversed based on the same rationale explained above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Shin-Hon Chen/

Primary Examiner, Art Unit 2431

Conferees:

Hai Tran

/Hai Tran/

Supervisory Patent Examiner, TC2400/4100

Kaveh Abrishamkar

/Kaveh Abrishamkar/

Primary Examiner, AU 2431